ALSD Local 106 (Rev. 07/13) Application for a Search Warrant

UNITED STATES DISTRICT COURT

for the

Southern District of Alabama

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)
(1) TOSHIBA LAPTOP COMPUTER, SERIAL NUMBER 69169379Q; (1) TOSHIBA LAPTOP COMPUTER, SERIAL NUMBER 9B281331K; and (1) CELLULAR TELEPHONE, MAKE APPLE, MODEL, I-PHONE 10XS, CURRENTLY LOCATED AT THE FBI MOBILE EVIDENCE ROOM LOCATED AT 200 N. ROYAL STREET, MOBILE, ALABAMA 36603

Case No. 19-MJ-00078-N

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location)*:

for further description, see Attachment A

located in the Southern District of Alabama, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B.

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. § 1343	Wire Fraud
18 U.S.C. § 1033	Insurance Fraud

The application is based on these facts:

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of days (give exact ending date if more than 30 days:) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

[redacted]

Printed name and title

Sworn to before me and attestation acknowledged pursuant to FRCP 4.1(b)(2).

Date:

U.S. Magistrate Judge
Katherine P. Nelson

Digitally signed by U.S. Magistrate Judge Katherine P. Nelson
DN: cn=U.S. Magistrate Judge Katherine P. Nelson, ou=Federal Judiciary, ou=U.S. Government, email=efile_nelson@alsd.uscourts.gov, c=US
Date: 2019.04.05 14:53:40 -06'00'

Judge's signature

City and state: Mobile, Alabama

KATHERINE P. NELSON, United States Magistrate Judge

Printed name and title

AFFIDAVIT IN SUPPORT OF AN APPLICATION UNDER RULE 41 FOR A WARRANT TO SEARCH AND SEIZE

I, [redacted], being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the examination of property, namely, three (3) electronic devices, which are currently in law enforcement possession, and the extraction of electronically stored information described in Attachment B.

2. I am a Special Agent with the Federal Bureau of Investigation. I am a law enforcement officer of the United States who is empowered by law to conduct investigations of and to make arrests for offenses against the United States. I have been employed by the FBI for 8 months. During my tenure with the FBI, I have been assigned investigations dealing with insurance fraud, wire fraud, identity theft, and public corruption. Through my training, education and experience, I have become familiar with the manner in which offenders communicate using e-mail, social media, and the internet to transmit, share or store evidence of crimes.

3. This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

4. To date, thirty-six grand jury subpoenas have been served to various banks and insurance carriers believed to have done business with Thomas E. Burns or Tommy Burns Agency, LLC. Additionally, several alleged victims and an employee of Tommy Burns Agency, LLC have provided some documents related to Thomas E. Burns and/or Tommy Burns Agency, LLC. While some documents received from these entities provide potential evidentiary value, they constitute an incomplete record of suspected illicit business dealings perpetrated by Thomas E. Burns. The warrant I apply for today would allow seizure of the additional information not yet obtained by investigators associated with this case.

PROBABLE CAUSE

1. On December 4, 2018, the Mobile Field Office of the Federal Bureau of Investigation received a walk-in complaint from Orange Beach, AL resident Katheryn Scott that Thomas Edward Burns dba Tommy Burns Agency, LLC was collecting insurance premiums from customers and not paying policy premiums to the underwriter, South Shore Insurance Underwriters (SSIU).

2. Katheryn Scott works as a part time accountant for SSIU and operates a business, Driftwood Investigations, LLC, as a certified fraud examiner. She previously worked as a forensic accountant for the Federal Bureau of Investigation in Mobile, AL. In October 2018, Katheryn Scott was contacted by her daughter, Mindy Dees, Marketing Director at SSIU, about a pattern of non-payment for policies by Tommy Burns Agency, LLC. SSIU was sending cancellation notices to customers of Burns due to the non-payment. Scott's internal investigation found that eight out of 16 policies bound by SSIU on behalf of Tommy Burns Agency were cancelled for non-payment.

3. On March 19, 2019, Dennis Wright from the Alabama Department of Insurance received a complaint against Tommy Burns Agency, LLC from CRC Insurance Services (CRC), parent company of Southern Cross Underwriters (SCU). The complaint detailed that SCU bound 20 policies for Tommy Burns Agency between November 2018 and February 2019 for a total of $24,329.00 in premiums. As of March 18, 2019, 17 of the policies had not been paid and had cancellations issued or expected to be issued. SCU filed the complaint after being contacted by several customers of Tommy Burns complaining that they had made full payment to Tommy Burns.

4. On March 21, 2019, I interviewed Carolyn Genry. She had a homeowner's policy paid via escrow to Tommy Burns Agency, LLC. She had received a cancellation notice from SCU. When she called SCU, she was told she was not able to get her policy reinstated due to non-payment. Mrs. Genry confronted Tommy Burns requesting a refund so that she could get a policy elsewhere. Mr. Burns did not offer a refund but offered to find Mrs. Genry insurance with another underwriter.

5. On March 22, 2019, I telephonically interviewed Melisa Hallmark, the Vice President of Agency Appointments and Administration with CRC Insurance Services (CRC), the parent company of Southern Cross Underwriters (SCU). Prior to March 18, 2019, several insured customers called the SCU office in Mississippi after having received policy cancellation notices. This was abnormal because SCU did not normally deal directly with insured. SCU is a brokerage that collected payments from agents and placed them with insurance exchanges. All the insured individuals that contacted SCU had applied for policies through Tommy Burns Agency, LLC. Each claimed they made full payments to Burns. SCU had 12 policies pending cancellation for

non-payment of premiums with five more expected to be issued. The total unpaid premiums before commission was $16,983.32. SCU communicated via email with the Tommy Burns Agency, LLC at tommy@tommyburnsagency.com. Tommy Burns Agency, LLC received a written notice from SCU sent on March 4, 2019 detailing 16 out of 19 accounts past due totaling $19,013.56.

6. On March 22, 2019, Special Agent [redacted] and I interviewed Wanda Stewart Turner (Turner). Turner is the daughter of Barkley Stewart (Stewart), aged 91. On December 26, 2018, Turner and Stewart visited Tommy Burns Agency, LLC and met with Burns. Stewart agreed to a home owner's insurance policy for one year. Turner wrote a check on Stewart's behalf to Tommy Burns Agency, LLC for $1053.96. In late January or early February 2019, Stewart received a letter in the mail from Southern Cross, the insurance underwriter that had bound the homeowner's policy from Burns. The letter stated that Stewart's policy was being cancelled for non-payment. In mid-February 2019, Turner made contact with Burns on the phone and Burns promised to write a check to SCU that day. Burns did write a check the following day. However, an SCU representative later told Turner that the check had bounced and Stewart's policy was cancelled. Turner filed a police report with the Mobile County Sheriff's Office.

7. On March 25, 2019, Special Agent [redacted] and I interviewed William Henry Couch, Junior (Couch). On September 19, 2018, Couch had a check from his Wells Fargo escrow account sent to Tommy Burns Agency, LLC in the amount of $1688.42 for insurance coverage. That check was cashed by Burns on September 24, 2018. In October 2018, Couch received a cancellation notice from South Shore Insurance Underwriters (SSIU) stating that his policy would be cancelled for non-payment effective November 3, 2018. Couch sent an email to Burns at tommy@tommyburnsagency.com on November 8, 2018 questioning why his policy was

cancelled. Couch demanded a cash refund, which Burns provided later that day at Couch's place of work, but only after Burns made Couch sign a document that he would not hold Burns liable for any losses resulting from the policy cancellation. Couch moved his policy to Ryan Reid Agency and paid SSIU directly to get his policy back in force. Couch provided Agents with printouts of emails from Burns to Couch using email address: tommy@tommyburnsagency.com, an escrow statement, and a cancellation letter in support of his allegations.

8. On March 25, 2019, Special Agent [redacted] and I interviewed Michael Dennis Hardy (Hardy), a friend of Thomas Burns, who has known him for about one year. In October 2018, Burns provided Hardy a homeowner's insurance quote that was almost half of what Hardy had previously paid for similar coverage. The quote was through South Shore Insurance Underwriters (SSIU). Hardy wrote Burns a check for $1197.78 on 10/11/2018. The policy was for one year of homeowner's insurance coverage. Hardy later learned from Tommy Burn's office assistant, Angela Bassett (Bassett), that Burns cashed his check at the Century Bank adjacent to Burn's office within minutes of Hardy departing. Hardy obtained a copy of the cashed check from the bank, which was endorsed by Burns on the back of the check. Several months later, Hardy received a notice of cancellation letter in the mail from SSIU. Hardy contacted SSIU and spoke to Mindy Dees (Dees). Dees told Hardy that SSIU had never received payment for his homeowner's insurance policy and, therefore, was canceling the policy for non-payment. Dees also told Hardy that SSIU no longer did business with Burns. Burns told Hardy that he would move his policy to a new company, SCU. However, Hardy never filled out any applications or other documents for SCU. Hardy later contacted SCU and learned that his homeowner's policy with them was only valid through March 31, 2019.

9. On March 26, 2019, Special Agent [redacted] and I met with Angela Kay McConnell Bassett (Bassett). Bassett currently serves as the office assistant at Tommy Burns Agency, LLC. Besides Burns, Bassett is the only other employee of Tommy Burns Agency, LLC. Bassett began working there in early October 2018. Bassett had no prior knowledge of the insurance business, so she relied on Burns to teach her. Bassett knew that Burns had recently began moving a number of insurance policies from Swyfft to South Shore Insurance Underwriters (SSIU). In late October or early November 2018, one of Burns' SSIU customers named Hank Thompson (Thompson) suffered a grease fire in his home kitchen. Thompson had paid Burns for a one-year homeowner's insurance policy through SSIU. However, Burns had not passed on the payment to SSIU. Shortly before the fire, SSIU had cancelled Thompson's insurance policy for non-payment. After Thompson notified Burns of the fire and his need to file a claim, Bassett overheard Burns call a representative at SSIU and ask for Thompson's policy to be reinstated with no loss of coverage. During this phone conversation, Burns did not inform SSIU that Thompson had suffered a kitchen fire and that a claim would be forthcoming. Burns paid the money owed on the policy in order to get it reinstated. SSIU agreed to reinstate the policy, but only beginning at 12:01am the following day. The next morning, Burns attempted to submit a claim on Thompson's behalf for the kitchen fire. On the claim, Burns changed the date of the fire to ensure Thompson would be covered. Bassett also overheard Burns telephone conversation to the Grand Bay fire department and convinced them that the fire had actually occurred on a different day, resulting in them issuing an amended report of the fire that falsely represented the actual date of the fire.

10. After this incident, Bassett began to notice that Burns often cashed checks received

from customers that was supposed to be for their insurance premiums, but Burns was not forwarding the money on to the insurance underwriters. Burns would often walk next door from the office to the Century Bank and cash the checks there. Burns would also go to the banks where the customers had their accounts to cash the checks. In November 2018, Burns directed Bassett to get new policies for all of his SSIU customers, because SSIU had cut him off. Burns had Bassett get new quotes from a different insurance underwriter, create falsified statements of no loss, and generate new policies. Burns then directed Bassett to sign the customer's name on the new policy applications. Burns told Bassett that it was fine and normal to switch the customer's insurance carrier and that the customer did not need to know. According to Bassett, the paper documents associated with these transactions were most likely shredded after they were saved and uploaded to the Microsoft OneDrive account from EZlinks, a software program that organizes files. Bassett indicated that any remaining paper documentation would be located at the Business.

11. Despite moving to new insurance underwriters, after about 60 days the insurance underwriters still had not been paid and began sending out cancellation notices for non-payment. From November 2018 through the present, Bassett stated that more and more customers have come to the office to demand their money back, as they had received cancellation notices in the mail. In one recent month, Burns took in over $20,000 in premium payments from customers, but did not pass any of it on to insurance underwriters. Bassett is maintaining an active list of people that she believes Burns has stolen from. About three weeks ago, Bassett started turning away new customers for fear that they too would be victimized by Burns. Without Burn's knowledge, Bassett told these individuals that they could not take on any new business and recommended other insurance agents in the area.

12. From my interview with Bassett and from reviewing documents received via subpoena, I learned that the following individuals and businesses paid their insurance premiums to the Tommy Burns Agency, but received notices of nonpayment or cancellation notices for nonpayment: Carolyn Genry, Blakely Lamar Stewart, Michael Hardy, Albert Pattat, Charles Mercer, Henry Thompson, William Couch, Jr., Michelle Pujols, Jon Custer, Johnny Shepherd, Gerald Capps, Gloria Capps, Christopher Taylor, Calvin Calhoun, Dan Riley, Joseph Spicciani, Jane Spicciani, Shane Sigsbee, Karen Leasure, Nino Mondaini, Samantha Alspaugh, Amy Switzer, Lynda Barker, Aleta Boudreaux, Mark Hale, Traci Hale, Pat Richards, Joseph McGugin, Latasha Schultz, Thurman Kittrell, John Kittrell, Christine McGallagher, Michael Mallini, Michaela Holloway, Christopher Hayes, FOGAB Marine Services, Spicy Group, LLC, Citizens for a Better Grand Bay Library and Museum, and Amy Spitzer Properties. Basset indicated that the documents associated with these customers was stored into Burns' Microsoft OneDrive account. While working at the Business, Burns directed Bassett to scan all documents into the Microsoft OneDrive account that Burns uses to store records and information related to Tommy Burns Agency, LLC. Many documents are also copied to the Microsoft OneDrive account from EZlinks, a software program that organizes files. Burns has told Bassett to shred everything once the documents have been scanned and uploaded. Bassett believes that Burns does not want to leave a paper trail and believes that he would begin deleting files if he thought law enforcement were on to him. Burns also directed Bassett to stop issuing receipts to customers who pay in cash. Bassett indicated that there is an excel spreadsheet to record payments (by both cash and check) received by customers. This excel spreadsheet is saved on Bassett's HP computer located at the on the Premises. Burns has not shared the Microsoft OneDrive account password with Bassett, but the account is always

logged in on Bassett's desktop computer on her desk at the office. Burns accesses the same Microsoft OneDrive account from the gray HP laptop on his desk at work. In addition, Bassett indicated that Burns possessed at least two additional laptops and an Apple iPhone cellular telephone that he carries with him when he leaves the Premises. Bassett stated that he often does business from his cellular phone and that he has access all of the business records on OneDrive by using his cellular phone which is associated with telephone number 251[redacted] Burns receives emails related to the Tommy Burns Agency, LLC on this cellphone. Many individuals often carry their cellular telephones on their person.

13. Burns drives a silver 2019 Toyota Camry, which he recently leased after totaling his previous vehicle in a single vehicle accident. He uses this vehicle to transport his phone and a laptop (unidentified make and model) to and from work. Burns' rarely arrives at the Business prior to 11:00am. Bassett stated that Burns showed up for work on Monday, March 25, 2019, but that was the first time Burns had been to the Premises on a Monday in several months. According to Bassett, Burns has spent less and less time at work as the number of customer's seeking refunds has grown, but continues to run the business from his phone and his laptop that he transports home with him. Burns did spend several hours at the Premises on March 26, 2019. However, Burns did not come to the Premises on March 27, 2019. Throughout March 27th, Burns continued to call and text from his telephone number 251-[redacted] which is the personal cellular number he provided to Bassett, and send her email from his email accounts tommy@tommyburnsagency.com, [redacted]@gmail.com, and [redacted]@yahoo.com, from his home at 8950 Spring Grove South, Mobile, AL 36695. In these communications, Burns directed Bassett to submit several new insurance policy applications on behalf of customers without their knowledge and

consent to a new insurance underwriter. Bassett did not submit the policies as directed.

14. On March 28, 2019, Special Agent [redacted] and I again met with Angela Bassett. The meeting occurred at the Premises where the business of Tommy Burns Agency, LLC is operated. Bassett provided several documents and additional information. The documents included a physical copy of an excel spreadsheet. The spreadsheet was a partial list of Tommy Burns Agency, LLC customers who had paid for insurance policies through Tommy Burns Agency, LLC. Bassett used this document to record payments received. The current, digital copy of this Excel spreadsheet is saved on the desktop folder of Bassett's HP desktop computer located at her desk. Bassett stated that all customers, with one exception, listed on the spreadsheet that had homeowner's insurance through Tommy Burns Agency, LLC had paid their premium for the policies, but Burns had not forwarded the money to the appropriate insurance underwriter.

15. Bassett also provided a copy of a letter from CRC Group, the parent company of SCU, with a list of nine insurance policies that were listed as past due and subject to cancellation. Bassett stated that all of the listed individuals had paid Burns for their policies, but Burns had failed to pass on the payments to SCU, except in one case.

16. On April 4, 2019, Special Agent [redacted] and I interviewed a local law enforcement officer with the Mobile County Sheriff's Office who was present during the service of a state arrest warrant for Burns on unrelated charges at Burns' home located at [redacted] Mobile, Alabama 36695. During service of the arrest warrant, local law enforcement from Mobile County Sheriff's Office saw drug paraphernalia in plain view. The deputies on scene obtained a search warrant for drugs at [redacted] During the course of that search, deputies found in plain view insurance policy documents as well as two laptop computers and a

cellular phone. Burns provided the passcode to unlock the cellular phone to the deputies. The laptops and cellular phone matched the description given by Bassett of those items that Burns would use for conducting the business of Tommy Burns Agency, LLC and had taken home with him. During the search of the home, deputies seized two (2) lap top computers and the cellphone of Tommy Burns. These electronic devices have now been turned over to the Federal Bureau of Investigation pending the issuance of the search warrant requested herein.

17. Based on my training, experience, and what I have learned from other law enforcement professionals, the affiant submits there is probable cause to believe electronically stored evidence and instrumentalities of the crimes of violation Title 18 USC § 1343, Wire Fraud and Title 18 USC § 1033, Insurance Fraud is contained on the electronic devices identified as belonging to Thomas Edward Burns and Tommy Burns Agency, LLC, to include, but not limited to, communications with clients, insurance applications, cancellation notices, payment records and bank and/financial records related to the deposit of premiums.

18. I hereby state that upon oath that the foregoing information is true to the best of my knowledge and belief.

19. I seek this warrant to be certain that the seizure and examination of the devices will comply with the Fourth Amendment and other applicable laws.

TECHNICAL TERMS

5. Based on my training and experience, I use the following technical terms to convey the following meanings:

a. IP Address: The Internet Protocol address (or simply "IP address") is a unique numeric address used by computers on the Internet. An IP address looks like a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

b. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

c. Storage medium: A storage medium is any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory/thumb drives, CD-ROMs, and other magnetic or optical media.

COMPUTERS, ELECTRONIC STORAGE, AND FORENSIC ANALYSIS

6. As described above and in Attachment B, this application seeks permission to search for records that might be found on the PREMISES, in whatever form they are found. One

form in which the records might be found is data stored on a computer's hard drive or other storage media. Thus, the warrant applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

7. *Probable cause.* I submit that if a computer or storage medium is found on the PREMISES, there is probable cause to believe those records will be stored on that computer or storage medium, for at least the following reasons:

a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

c. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

e. Based on actual inspection of other evidence related to this investigation, including spreadsheets, financial records, and insurance policy applications, I am aware that computer equipment was used to generate, store, and print documents used in the wire and insurance fraud schemes. There is reason to believe that there is a computer system currently located on the PREMISES.

8. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable

cause to believe that this forensic electronic evidence will be on any storage medium in the PREMISES because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.

b. As explained herein, information stored within a computer and other electronic storage media may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (e.g., registry information,

communications, images and movies, transactional information, records of session times and durations, internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculpating or exculpating the computer owner. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, as described herein, computers typically contain information that log: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs,

may also indicate the presence of additional electronic storage media (e.g., a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculpate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (e.g., internet searches indicating criminal planning), or consciousness of guilt (e.g., running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves.

Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

f. I know that when an individual uses a computer to transmit falsified, forged, or unauthorized documents, the individual's computer will generally serve both as an instrumentality for committing the crime, and also as a storage medium for evidence of the crime. The computer is an instrumentality of the crime because it is used as a means of committing the criminal offense. The computer is also likely to be a storage medium for evidence of crime. From my training and experience, I believe that a computer used to commit a crime of this type may contain: data that is evidence of how the computer was used; data that was sent or received; notes as to how the criminal conduct was achieved; records of Internet discussions about the crime; and other records that indicate the nature of the offense.

9. *Necessity of seizing or copying entire computers or storage media.* In most cases, a thorough search of a premises for information that might be stored on storage media often requires the seizure of the physical storage media and later off-site review consistent with the

warrant. In lieu of removing storage media from the premises, it is sometimes possible to make an image copy of storage media. Generally speaking, imaging is the taking of a complete electronic picture of the computer's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

a. The time required for an examination. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine storage media to obtain evidence. Storage media can store a large volume of information. Reviewing that information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.

b. Technical requirements. Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or

knowledge will be required to analyze the system and its data on the Premises. However. taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.

c. Variety of forms of electronic media. Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

10. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise copying storage media that reasonably appear to contain some or all of the evidence described in the warrant, and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

CONCLUSION

11. I submit that this affidavit supports probable cause for a warrant to search the property identified in Attachment A and seize the items described in Attachment B.

Respectfully submitted,

[redacted]
Special Agent
Federal Bureau of Investigation

THE ABOVE AGENT HAD ATTESTED TO THIS AFFIDAVIT PURSUANT TO FED. R. CRIM. P. 4.1(b)(2)(B) THIS _____ DAY OF APRIL 2019.

U.S. Magistrate Judge Katherine P. Nelson

Digitally signed by U.S. Magistrate Judge Katherine P. Nelson
DN: cn=U.S. Magistrate Judge Katherine P. Nelson, o=Federal Judiciary, ou=U.S. Government, email=efile_nelson@alsd.uscourts.gov, c=US
Date: 2019.04.05 14:55:44 -06'00'

KATHERINE P. NELSON
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

Property to be searched

The property to be searched are the following (hereafter referred to as devices):

Type:	Laptop Computer
Make:	Toshiba
Model:	S/N 69169379Q
Type:	Laptop Computer
Make:	Toshiba
Model:	S/N 9B281331K
Type:	Cellular telephone
Make:	Apple
Model:	iPhone 10XS

This devices are currently located at the FBI Mobile Evidence Control Room located at 200 N. Royal Street, Mobile, AL 36603. This warrant authorizes the forensic examination of the devices for the purpose of identifying the electronically stored information described in Attachment B.

ATTACHMENT B

Property to be seized

1. All records on the devices described in Attachment A relating to violations of Title 18 U.S.C. § 1343, Wire Fraud and Title 18 U.S.C. § 1033, Insurance Fraud, those violations involving Thomas Edward Burns and/or Tommy Burns Agency, LLC and occurring after November 8, 2016 (the date in which the Tommy Burns Agency, LLC received its insurance license) including:

   a. Records and information relating to insurance policies, policy applications, cancellation notices, customer requests for refunds of their policy premiums and other client communication, customer payment information, financial documents showing deposits of client premiums, checks or copies of checks to/from clients, escrow services and insurance underwriter information.. Records and information relating to the following e-mail accounts used by Burns: tommy@tommyburnsagency.com, [redacted]@yahoo.com, and [redacted]@gmail.com;

   b. Records and information relating to the tracking of payments, payment logs, cancellation notices for non-payment of premiums, policy applications, requests for refunds of premiums, receipts for premium payments, invoices for payments, documents showing deposits of client premiums, checks or copies of checks to or from clients, escrow services, and insurance underwriters;

c. Records and information relating to any agreements, contracts, or communication that may exist or existed between Thomas E. Burns and/or Tommy Burns Agency, LLC and the individuals/entities identified herein as well as any other individual or business who has received a notice of nonpayment or cancellation notice due to nonpayment from November 1, 2018 through the present;

d. Records and information relating to all customers who had policies quoted or bound through Thomas E. Burns and/or Tommy Burns Agency, LLC from November 1, 2018 to the present;

e. Records and information relating to any complaints relating to policies bound or issued by or through Tommy Burns Agency, LLC from November 1, 2018 to the present.

2. For any computer or storage medium whose seizure is otherwise authorized by this warrant, and any computer or storage medium that contains or in which is stored records or information that is otherwise called for by this warrant (hereinafter, "COMPUTER"):

a. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;

b. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

c. evidence of the lack of such malicious software;

d. evidence indicating how and when the computer was accessed or used to determine the chronological context of computer access, use, and events relating to crime under investigation and to the computer user;

e. evidence indicating the computer user's state of mind as it relates to the crime under investigation;

f. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;

g. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER;

h. evidence of the times the COMPUTER was used;

i. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;

j. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;

k. records of or information about Internet Protocol addresses used by the COMPUTER;

l. records of or information about the COMPUTER's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses;

m. contextual information necessary to understand the evidence described in this attachment.

As used above, the terms "records" and "information" includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

The term "computer" includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

The term "storage medium" includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory/thumb drives, CD-ROMs, and other magnetic or optical media.

This warrant authorizes a review of electronic storage media and electronically stored information seized or copied pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the seized or copied electronic data to the custody and control of attorneys for the government and their support staff for their independent review.